AMENDMENTS TO THE CLAIMS

1-28 (Canceled).

29.   (Currently Amended) A method comprising:

for each electronic device of a plurality of electronic devices, in real time:

receiving, in a backend system, information related to digital data captured by the electronic device at a transport layer before the digital data is provided to an application layer for presentation to a user of the electronic device, the backend system comprising at least one server;

on the at least one server, determining a digital-data rating via the information related to the captured digital data, the determining comprising:

checking a ratings database for a pre-existing rating for the captured digital data using a network address included in the information related to the captured digital data;

responsive to the network address being found in the ratings database, using the pre-existing rating as the digital-data rating;

responsive to the captured digital data not being found in the ratings database:

crawling the captured digital data via the network address;

accessing the captured digital data over a ~~the~~ network;

performing a word-by-word analysis of the captured digital data to determine the digital-data rating; and

updating the ratings database with the network address and the digital-data rating responsive to the performance of the word-by-word analysis;

designating the captured digital data as illicit digital data or non-illicit digital data, the designating comprising designating the captured digital data as illicit digital data if the digital-data rating exceeds a predetermined threshold; and

transmitting a result of the designating from the at least one server to the electronic device to block the illicit digital data from delivery to the application layer.

30.   (Previously Presented)   The method of claim 29, comprising, for each of the plurality of electronic devices, in real time, allowing delivery of the non-illicit digital data to the application layer for presentation to the user of the electronic device.

31.   (Previously Presented)   The method of claim 29, comprising, for each of the plurality of electronic devices, in real time, capturing all requests for digital data over the network by the electronic device.

32.   (Previously Presented)   The method of claim 31, comprising:

for each of the plurality of electronic devices, concurrently routing:

information relating to at least some of the captured requests for digital data to the at least one server providing the content-rating service; and

the at least some captured requests to intended destinations on the network.

33.   (Previously Presented)   The method of claim 32, wherein at least some of the captured digital data is digital data received at the electronic device as a result of the step of routing the information relating to at least some of the captured requests for digital data to the intended destinations.

34.   (Previously Presented)   The method of claim 32, wherein at least some of the captured digital data is digital data received at the electronic device independent of the routing step.

35.   (Previously Presented)   The method of claim 32, comprising, on the at least one server:

crawling requested digital data on the network using the at least some of the captured requests; and

rating the requested digital data for illicitness using a word-by-word analysis of the requested digital data.

36.   (Previously Presented)   The method of claim 35, further comprising, responsive to the rating step, storing a rating and identification information for the rated digital data together in a content database in communication with the at least one server.

37.   (Previously Presented)   The method of claim 29, comprising, for each of the plurality of electronic devices, sending an authentication signal to the backend system, the authentication signal providing validation information indicating whether the electronic device corresponds to a valid user account.

38.   (Previously Presented)   The method of claim 29, further comprising, for each of the plurality of electronic devices, filtering communication between the electronic device and the network for personal information.

39.   (Previously Presented)   The method of claim 29, further comprising, for each of the plurality of electronic devices, filtering communication between the electronic device and the network for explicit requests for illicit content.

40.   (Previously Presented)   The method of claim 29, wherein the electronic device comprises at least one of:
    a personal computer;
    a set-top box;
    a router; and
    a gateway.

41.   (Previously Presented)   The method of claim 35, further comprising transmitting configuration settings to the electronic device corresponding to the valid user account.

42.   (Previously Presented)   The method of claim 29, wherein at least some of the captured digital data comprises an instant message en route to an instant messaging application on the electronic device.

43.   (Previously Presented)   The method of claim 29, wherein at least some of the captured digital data comprises an email message en route to an email application on the electronic device.

44.   (Previously Presented)   The method of claim 29, further comprising, for at least one of the electronic devices, rating the captured digital data for illicitness utilizing a content-rating module on the electronic device.

45.   (Previously Presented)   The method of claim 29, comprising, for at least one of the plurality of electronic devices:

        transmitting information related to the captured digital data to a reporting server; and

        on the reporting server, logging network activities of the user of the electronic device via the information related to the captured digital data.

46.   (Previously Presented)   The method of claim 45, comprising:

        on the reporting server, for the at least one of the plurality of electronic devices:

                generating a report summarizing illicitness of network activities of the user of the electronic device for a predetermined time period; and

                transmitting the report over the network to a third party.

47.   (Previously Presented)   The method of claim 45, comprising:

        wherein the at least one of the plurality of electronic devices comprises more than one electronic device;

                generating a multi-user report summarizing illicitness of network activities of each user of the more than one electronic device for a predetermined time period; and

5

transmitting the multi-user report over the network to a third party.

48.   (Previously Presented)   The method of claim 29, comprising, for at least one of the plurality of electronic devices:

transmitting an indication from the backend system to the at least one of the plurality of electronic devices on whether the captured digital data is malicious or non-malicious; and

blocking the captured digital data deemed to be malicious.

49.   (Previously Presented)   The method of claim 31, comprising, for at least one of the plurality of electronic devices:

transmitting an indication from the backend system that at least one of the captured requests for digital data represents an unauthorized intrusion on the electronic device; and

denying the at least one of the captured requests for digital data.

50.   (Canceled).

51.   (Previously Presented)   A method comprising:

for each electronic device of a plurality of electronic devices, in real time:

on the electronic device, at a transport layer, capturing all digital data received by the electronic device over a network before the digital data is provided to an application layer for presentation to a user of the electronic device;

routing information related to the digital data to a backend system on the network, the backend system comprising at least one server, the at least one server providing a content-rating service for rating digital-data illicitness;

delaying delivery of the digital data to the application layer on the electronic device at least until the digital data is designated non-illicit by the at least one server;

on the at least one server, determining a digital-data rating via the information related to the digital data, the determining comprising:

checking a ratings database for a pre-existing rating for the digital data using a network address included in the information related to the digital data;

6

responsive to the network address being found in the ratings database,
using the pre-existing rating as the digital-data rating;

responsive to the digital data not being found in the ratings database:

crawling the digital data via the network address;

accessing the digital data over the network;

performing a word-by-word analysis of the digital data to
determine the digital-data rating; and

updating the ratings database with the network address and the
digital-data rating responsive to the performance of the word-by-word analysis;

designating the digital data as illicit digital data or non-illicit digital data,
the designating comprising designating the digital data as illicit digital data if the digital-data
rating exceeds a predetermined threshold;

on the electronic device, receiving the designation from the at least one server;
and

on the electronic device, blocking the illicit digital data from delivery to the
application layer.

52.   (Currently Amended) An article of manufacture, the article of manufacture
comprising:

at least one computer-readable medium;

processor instructions contained on the at least one computer readable medium, the
processor instructions configured to be readable from the at least one computer-readable medium
by at least one processor and thereby cause the at least one processor to operate as to, for each of
a plurality of electronic devices, in real time:

receive, in a backend system, information related to digital data captured by the
electronic device at a transport layer before the digital data is provided to an application layer for
presentation to a user of the electronic device, the backend system comprising at least one server;

on the at least one server, determine a digital-data rating via the information
related to the digital data, the determining comprising:

7

check a ratings database for a pre-existing rating for the digital data using a network address included in the information related to the digital data;

responsive to the network address being found in the ratings database, use the pre-existing rating as the digital-data rating;

responsive to the digital data not being found in the ratings database:

crawl the digital data via the network address;

access the digital data over a ~~the~~ network;

perform a word-by-word analysis of the digital data to determine the digital-data rating; and

update the ratings database with the network address and the digital-data rating responsive to the performance of the word-by-word analysis;

designate the digital data as illicit digital data or non-illicit digital data, the designating comprising designating the digital data as illicit digital data if the digital-data rating exceeds a predetermined threshold; and

transmit the designation from the at least one server to the electronic device so that the electronic device may block the illicit digital data from delivery to the application layer.

8